

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-072872

(43)Date of publication of application : 12.03.2002

(51)Int.Cl.

G09C 1/00

(21)Application number : 2000-259853

(71)Applicant : NTT COMWARE CORP

(22)Date of filing : 29.08.2000

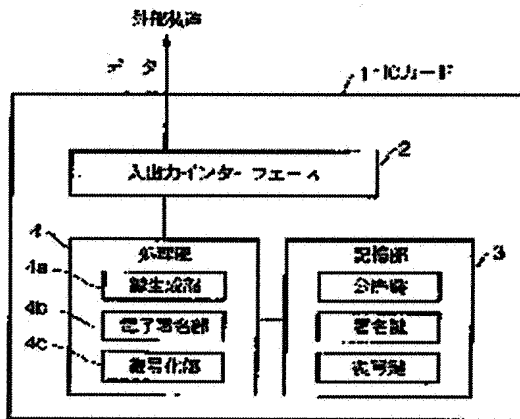
(72)Inventor : FURUKAWA YOSHISATO

(54) DEVICE AND METHOD FOR SECURING DATA, AND RECORDING MEDIUM THEREOF

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an enciphering system and an electronic signature system for company use.

SOLUTION: A data security device of this invention has three keys of one public key in accordance with a public key system, a signature key to be used for electronically signing a plain text together with this public key, and a decoding key for decoding the cryptogram enciphered by the public key differing from this signature key. The data security device of this invention is especially packaged as an IC, and the decoding key is separately kept by an organization for managing it.



対応なし、英抄

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-72872

(P2002-72872A)

(43) 公開日 平成14年3月12日 (2002.3.12)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 A 5 J 1 0 4
	6 2 0		6 4 0 Z
			6 2 0 B

審査請求 有 請求項の数10 O L (全 11 頁)

(21) 出願番号 特願2000-259853(P2000-259853)

(22) 出願日 平成12年8月29日 (2000.8.29)

(71) 出願人 397065480

エヌ・ティ・ティ・コムウェア株式会社
東京都港区港南一丁目9番1号

(72) 発明者 古川 嘉識

東京都港区港南一丁目9番1号 エヌ・ティ・ティ・コミュニケーションウェア株式会社内

(74) 代理人 100064908

弁理士 志賀 正武 (外2名)

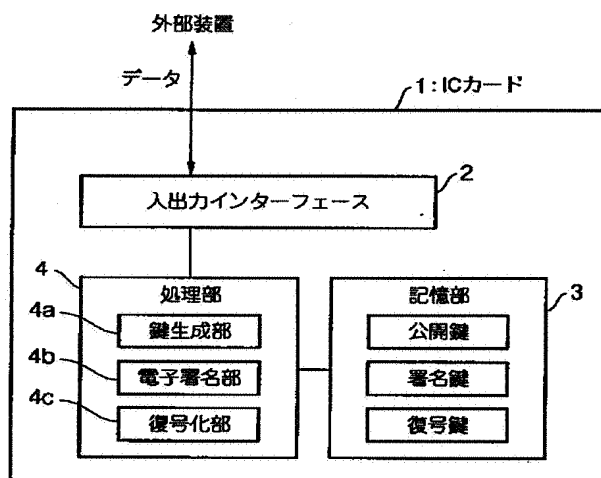
Fターム(参考) 5J104 AA09 JA23 LA03 LA06 NA02
NA35 NA37

(54) 【発明の名称】 データセキュリティ装置、データセキュリティ方法及びその記録媒体

(57) 【要約】

【課題】 本発明の目的は、企業ユースにおいて、より安全な暗号方式・電子署名方式を提供することにある。

【解決手段】 本発明のデータセキュリティ装置は、公開鍵方式による、1つの公開鍵と、この公開鍵とともに利用し平文の電子署名に用いる署名鍵と、この署名鍵とは異なり公開鍵で暗号化された暗号文の復号化に用いる復号鍵の3つの鍵をもつ。本発明のデータセキュリティ装置は、特に、ICカードとして実装され、復号鍵は、復号鍵を管理する機関に別途預託される。



【特許請求の範囲】

【請求項 1】 平文の暗号化および暗号文の復号化とさらに平文の電子署名をするために用いる装置において、前記装置は、

公開鍵方式による、1の公開鍵と、該公開鍵とともに利用し平文の電子署名に用いる第1の秘密鍵と、前記公開鍵で暗号化された暗号文の復号化に用いる第2の秘密鍵と、を有し、

前記第1の秘密鍵と第2の秘密鍵は異なるものであることを特徴とするデータセキュリティ装置。

【請求項 2】 前記データセキュリティ装置は、プログラム処理を行う処理部と、前記公開鍵と第1の秘密鍵と第2の秘密鍵を含むデータを記憶する記憶部と、データの入出力を行う入出力インターフェースと、を具備するICカードにより構成され、

前記処理部は、

電子署名に係る暗号化を、前記記憶部に記憶された第1の秘密鍵を用いて行い、

前記公開鍵により暗号化された暗号文の復号化を、前記記憶部に記憶された第2の秘密鍵を用いて行う、ことを特徴とする請求項 1 に記載のデータセキュリティ装置。

【請求項 3】 前記 IC カードの処理部は、

前記入出力インターフェースを介して、

該 IC カードに接続された外部装置に、前記公開鍵を出力し、

前記外部装置から電子署名の対象となるデータが入力されると、該入力されたデータを前記第1の秘密鍵を用いて暗号化し、該暗号化により得られた暗号文を前記外部装置に出力し、

前記外部装置から前記公開鍵を用いて暗号化された暗号文が入力されると、該入力された暗号文を前記第2の秘密鍵を用いて復号化し、該復号化により得られた平文を前記外部装置に出力することを特徴とする請求項 2 に記載のデータセキュリティ装置。

【請求項 4】 前記処理部は、

前記公開鍵と第1の秘密鍵と第2の秘密鍵を生成し前記記憶部に記憶させることを特徴とする請求項 3 に記載のデータセキュリティ装置。

【請求項 5】 前記公開鍵方式は、

2つの相異なる素数P1およびQ1を決定し、該P1およびQ1に対し、 $(P1-1) \times (Q1-1)$ と互いに素かつ $LCM(P1-1, Q1-1) \times n1+1$ 以外の自然数の列E1と、

前記P1およびQ1と異なるとともに相異なる2つの素数P2およびQ2を決定し、該P2およびQ2に対し、 $(P2-1) \times (Q2-1)$ と互いに素かつ $LCM(P2-1, Q2-1) \times n2+1$ 以外の自然数の列E2と、を求め、前記E1およびE2の共通部分 $E1 \cap E2$ から、任意の1つの自然数Eを決定し、

Eと $N1 = P1 \times Q1$ と $N2 = P2 \times Q2$ の組(E, N1, N2)を前記1の公開鍵とし、

等式： $E \times D1 = LCM(P1-1, Q1-1) \times n1+1$ を満たす自然数D1を決定し、D1およびN1の組(D1, N1)を第1の秘密鍵とし、

等式： $E \times D2 = LCM(P2-1, Q2-1) \times n2+1$ を満たす自然数D2を決定し、D2およびN2の組(D2, N2)を第2の秘密鍵とし、

電子署名の対象である平文に対応するデータM1に対し、第1の秘密鍵を用いて、その電子署名Sを、N1を法とし、

$S \equiv M1^{D1} \pmod{N1}$ 、とし、

該電子署名の確認を、公開鍵の要素であるEとN1を用いて、N1を法とし、

$M1' \equiv S^E \pmod{N1}$ 、を求め、該M1'がM1と一致することで電子署名の確認を行い、

平文M2に対し、公開鍵の要素であるEとN2を用いて、その暗号文Cを、N2を法とし、

$C \equiv M2^E \pmod{N2}$ 、として求め、
20 該暗号文Cの復号化を、前記第2の秘密鍵を用いて、N2を法とし、

$M2 \equiv C^{D2} \pmod{N2}$ 、より求めることを特徴とする請求項 1 ないし請求項 4 のいずれかに記載のデータセキュリティ装置。ただし、 $LCM(P1-1, Q1-1)$ は、 $(P1-1)$ と $(Q1-1)$ の最小公倍数であり、 $LCM(P2-1, Q2-1)$ は、 $(P2-1)$ と $(Q2-1)$ の最小公倍数であり、n1およびn2は任意の負でない整数である。

【請求項 6】 公開鍵の電子証明書において、前記公開鍵の第2要素N1と第3要素N2の一方を、ITU-T X.509バージョン3の拡張領域に格納することを特徴とする請求項 5 に記載のデータセキュリティ装置。

【請求項 7】 デジタルデータの安全を守るための方法において、

公開鍵方式による、1の公開鍵と、該公開鍵とともに利用し平文の電子署名に用いる第1の秘密鍵と、さらに、該第1の秘密鍵とは異なり前記公開鍵で暗号化された暗号文の復号化に用いる第2の秘密鍵と、を用い、

平文の電子署名を、前記第2の秘密鍵を用いて行い、

40 前記公開鍵により暗号化された暗号文の復号化を、前記第1の秘密鍵を用いて行うことを特徴とするデータセキュリティ方法。

【請求項 8】 請求項 7 に記載のデータセキュリティ方法において、

前記第2の秘密鍵を、該第2の秘密鍵を管理する鍵管理機関に預託し、

該第2の秘密鍵の所有者または該所有者より指定された者は、必要に応じて、該第2の秘密鍵を前記鍵管理機関より再取得可能とすることを特徴とするデータセキュリティ方法。

【請求項9】 プログラム制御回路を含むコンピュータ装置にインストールすることにより、該コンピュータ装置が請求項1に記載のデータセキュリティ装置を実現する装置となるソフトウェアが記録されたコンピュータ読取可能な記録媒体であって、

公開鍵方式による、1の公開鍵と、該公開鍵とともに利用し前記第1の秘密鍵とは異なり平文の電子署名に用いる第1の秘密鍵と、さらに、前記公開鍵で暗号化された暗号文の復号化に用いる第2の秘密鍵と、からなるデータと、

平文の電子署名に係る暗号化を、前記第1の秘密鍵を用いて行う手順と、

前記公開鍵により暗号化された暗号文の復号化を、前記第2の秘密鍵を用いて行う手順と、

をコンピュータに実行させるためのプログラムを記録した記録媒体。

【請求項10】 プログラム制御回路を含むコンピュータ装置にインストールすることにより、該コンピュータ装置が請求項1に記載のデータセキュリティ装置を実現する装置となるソフトウェアが記録されたコンピュータ読取可能な記録媒体であって、

公開鍵方式による、1の公開鍵と、該公開鍵とともに利用し平文の電子署名に用いる第1の秘密鍵と、さらに、前記第1の秘密鍵とは異なり前記公開鍵で暗号化された暗号文の復号化に用いる第2の秘密鍵と、を生成する手順と、

平文の電子署名に係る暗号化を、前記第1の秘密鍵を用いて行う手順と、

前記公開鍵により暗号化された暗号文の復号化を、前記第2の秘密鍵を用いて行う手順と、

をコンピュータに実行させるためのプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタルデータのセキュリティに係る暗号化および復号化ならびに電子署名に用いる装置および方法に関する。

【0002】

【従来の技術】従来の公開鍵暗号方式では、公開鍵と秘密鍵の2つの鍵を利用し、暗号化・復号化ならびに電子署名を実現している。

【0003】

【発明が解決しようとする課題】この公開鍵暗号方式では、公開鍵で暗号化された情報は秘密鍵でのみ復号化できる。もしこの秘密鍵を紛失してしまった場合、暗号化された情報は復号不可能となり失われてしまう。そのため企業ユースでは、社員の秘密鍵を預託という形で管理することが考えられている。一方、電子署名は、上記のように、秘密鍵で署名（暗号化）を行い、公開鍵で署名の確認を行うものである。この電子署名は、署名を行っ

た人物しか秘密鍵を知らない原則に基づいている。つまり秘密鍵の紛失に備えて預託を行えば電子署名に係る事後否認防止性が弱まり、事後否認防止のため秘密鍵を個人管理にすれば上記のように秘密鍵紛失と同時に情報を失う危険性が発生する（図6参照）。以上のように、従来の2つの鍵を用いた公開鍵暗号方式による、暗号化復号化および電子署名は、必ずしも安全なものとは言えない。

【0004】本発明は、上記の点に鑑みてなされたもので、企業ユースにおいて、より安全な暗号方式・電子署名方式を提供するものである。

【0005】

【課題を解決するための手段】本発明のデータセキュリティ装置は、平文の暗号化および暗号文の復号化とさらに平文の電子署名をするために用いる装置において、前記装置は、公開鍵方式による、1の公開鍵と、該公開鍵とともに利用し平文の電子署名に用いる第1の秘密鍵と、前記公開鍵で暗号化された暗号文の復号化に用いる第2の秘密鍵と、を有し、前記第1の秘密鍵と第2の秘密鍵は異なるものであることを特徴とする。

【0006】また、本発明のデータセキュリティ装置は、プログラム処理を行う処理部と、前記公開鍵と第1の秘密鍵と第2の秘密鍵を含むデータを記憶する記憶部と、データの入出力を行う出力インターフェースと、を具備するICカードにより構成され、前記処理部は、電子署名に係る暗号化を、前記記憶部に記憶された第1の秘密鍵を用いて行い、前記公開鍵により暗号化された暗号文の復号化を、前記記憶部に記憶された第2の秘密鍵を用いて行う、ことを特徴とする。

【0007】また、本発明のデータセキュリティ装置において、前記ICカードの処理部は、前記入出力インターフェースを介して、該ICカードに接続された外部装置に、前記公開鍵を出力し、前記外部装置から電子署名の対象となるデータが入力されると、該入力されたデータを前記第1の秘密鍵を用いて暗号化し、該暗号化により得られた暗号文を前記外部装置に出力し、前記外部装置から前記公開鍵を用いて暗号化された暗号文が入力されると、該入力された暗号文を前記第2の秘密鍵を用いて復号化し、該復号化により得られた平文を前記外部装置に出力することを特徴とする。

【0008】また、本発明のデータセキュリティ装置において、前記処理部は、前記公開鍵と第1の秘密鍵と第2の秘密鍵を生成し前記記憶部に記憶させることを特徴とする。

【0009】また、本発明のデータセキュリティ装置において、前記公開鍵方式は、2つの相異なる素数P1およびQ1を決定し、該P1およびQ1に対し、 $(P1-1) \times (Q1-1)$ と互いに素かつLCM $(P1-1, Q1-1) \times n1+1$ 以外の自然数の列E1と、前記P1およびQ1と異なるとともに相異なる2つの素数P2およびQ2

を決定し、該P2およびQ2に対し、 $(P2-1) \times (Q2-1)$ と互いに素かつ $LCM(P2-1, Q2-1) \times n2+1$ 以外の自然数の列E2と、を求め、前記E1およびE2の共通部分 $E1 \cap E2$ から、任意の1つの自然数Eを決定し、Eと $N1=P1 \times Q1$ と $N2=P2 \times Q2$ の組(E, N1, N2)を前記1の公開鍵とし、等式： $E \times D1 = LCM(P1-1, Q1-1) \times n1+1$ を満たす自然数D1を決定し、D1およびN1の組(D1, N1)を第1の秘密鍵とし、等式： $E \times D2 = LCM(P2-1, Q2-1) \times n2+1$ を満たす自然数D2を決定し、D2およびN2の組(D2, N2)を第2の秘密鍵とし、電子署名の対象である平文に対応するデータM1に対し、第1の秘密鍵を用いて、その電子署名Sを、N1を法とし、 $S \equiv M1^{D1} \pmod{N1}$ とし、該電子署名の確認を、公開鍵の要素であるEとN1を用いて、N1を法とし、 $M1' \equiv S^E \pmod{N1}$ を求め、該M1'がM1と一致することで電子署名の確認を行い、平文M2に対し、公開鍵の要素であるEとN2を用いて、その暗号文Cを、N2を法とし、 $C \equiv M2^E \pmod{N2}$ として求め、該暗号文Cの復号化を、前記第2の秘密鍵を用いて、N2を法とし、 $M2 \equiv C^{D2} \pmod{N2}$ より求めることを特徴とする。ただし、 $LCM(P1-1, Q1-1)$ は、 $(P1-1)$ と $(Q1-1)$ の最小公倍数であり、 $LCM(P2-1, Q2-1)$ は、 $(P2-1)$ と $(Q2-1)$ の最小公倍数であり、n1およびn2は任意の負でない整数である。

【0010】また、本発明は、公開鍵の電子証明書において、前記公開鍵の第2要素N1と第3要素N2の一方を、ITU-T X.509バージョン3の拡張領域に格納することを特徴とする。

【0011】また、本発明のデータセキュリティ方法は、デジタルデータの安全を守るための方法において、公開鍵方式による、1の公開鍵と、該公開鍵とともに利用し平文の電子署名に用いる第1の秘密鍵と、さらに、該第1の秘密鍵とは異なり前記公開鍵で暗号化された暗号文の復号化に用いる第2の秘密鍵と、を用い、平文の電子署名を、前記第2の秘密鍵を用いて行い、前記公開鍵により暗号化された暗号文の復号化を、前記第1の秘密鍵を用いて行うことを特徴とする。

【0012】また、請求項7に記載のデータセキュリティ方法において、前記第2の秘密鍵を、該第2の秘密鍵を管理する鍵管理機関に預託し、該第2の秘密鍵の所有者または該所有者より指定された者は、必要に応じて、該第2の秘密鍵を前記鍵管理機関より再取得可能とすることを特徴とする。

【0013】また、本発明は、プログラム制御回路を含むコンピュータ装置にインストールすることにより、該コンピュータ装置が請求項1に記載のデータセキュリティ装置を実現する装置となるソフトウェアが記録されたコンピュータ読取可能な記録媒体であって、公開鍵方式

による、1の公開鍵と、該公開鍵とともに利用し前記第1の秘密鍵とは異なり平文の電子署名に用いる第1の秘密鍵と、さらに、前記公開鍵で暗号化された暗号文の復号化に用いる第2の秘密鍵と、からなるデータと、平文の電子署名に係る暗号化を、前記第1の秘密鍵を用いて行う手順と、前記公開鍵により暗号化された暗号文の復号化を、前記第2の秘密鍵を用いて行う手順と、をコンピュータに実行させるためのプログラムを記録した記録媒体である。

【0014】また、本発明は、プログラム制御回路を含むコンピュータ装置にインストールすることにより、該コンピュータ装置が請求項1に記載のデータセキュリティ装置を実現する装置となるソフトウェアが記録されたコンピュータ読取可能な記録媒体であって、公開鍵方式による、1の公開鍵と、該公開鍵とともに利用し平文の電子署名に用いる第1の秘密鍵と、さらに、前記第1の秘密鍵とは異なり前記公開鍵で暗号化された暗号文の復号化に用いる第2の秘密鍵と、を生成する手順と、平文の電子署名に係る暗号化を、前記第1の秘密鍵を用いて行う手順と、前記公開鍵により暗号化された暗号文の復号化を、前記第2の秘密鍵を用いて行う手順と、をコンピュータに実行させるためのプログラムを記録した記録媒体である。

【0015】

【発明の実施の形態】以下、本発明の実施の形態を、図面を参照して説明する。図1は、本発明の一実施の形態であるICカードの構成を示すブロック図である。

【0016】ICカード1は、外部装置（図示せず）と接続されデータの入出力を行う入出力インターフェース2と、公開鍵暗号方式による公開鍵と署名鍵（第1の秘密鍵）と復号鍵（第2の秘密鍵）と一時データとを記憶する記憶部3と、下記の鍵生成部4aと電子署名部4bと復号化部4cとからなる処理部4とから構成される。

【0017】鍵生成部4aは、公開鍵暗号方式による公開鍵と復号鍵と署名鍵を生成し、記憶部3に記憶させる。電子署名部4bは、署名鍵を用いて、電子署名のために、対象となる平文に対応するデータの暗号化をする。署名鍵を用いて暗号化されるデータの入力および暗号化されたデータの出力は、入出力インターフェース2を介して行われる。復号化部4cは、復号鍵を用いて、公開鍵により暗号化された暗号文を復号化する。そして、復号化した結果の平文を、入出力インターフェース2を介して外部装置に出力する。なお、この公開鍵は、入出力インターフェース2を介して外部装置に出力（提供）され、外部装置によりこの公開鍵を使って平文の暗号化がなされる。

【0018】なお、記憶部3は、RAM(Random Access Memory)等の揮発性の記憶素子により構成されている。また、この処理部4はメモリおよびCPU(中央演算装置)等により構成され、処理部4

の各機能を実現するためのプログラム（図示せず）をメモリにロードして実行することによりその機能が実現されるものとする。また、このプログラムは、ROM（Read Only Memory）等の不揮発性の記憶素子（図示せず）に記憶されているものとする。

【0019】次に、このように構成された本実施の形態のICカード1の動作について、図2～4を参照して説明する。

【0020】まず、はじめに、鍵生成部4aは、公開鍵暗号方式に基づく公開鍵と復号鍵と署名鍵を生成し（図3：①、図4（a）：①）、記憶部3に記憶させる（図2：ステップS1）。なお、ここで生成する3つの鍵生成の具体例は後述する。次に、処理部4は、ICカード1が接続された外部装置からの要求により、記憶部3から公開鍵を読み出し、入出力インターフェース2を介して外部装置へ出力する（図3：②、図4（a）：②、図2：ステップS2）。同様に、処理部4は、外部装置からの要求により、記憶部3から復号鍵を読み出し、入出力インターフェース2を介して外部装置へ出力する（図2：ステップS3）。

【0021】なお、出力された公開鍵は、認証機関（CA）により証明書（X.509証明書）という形で、他のユーザに公開される（図3：④）。また、復号鍵は、秘密鍵を管理する所定の鍵管理機関に預託され別途管理される（図3：③、図4（a）：③）。一方、署名鍵は、ICカード1の外部に出力されることはない。これらにより、ICカード1の紛失や破壊によって復号鍵の失ったとしても、上記鍵管理機関において保管された復号鍵を用いて、対応する公開鍵により暗号化された暗号文の復号化を実施することが可能となる。また、署名鍵は、ICカード1の外部に出力されることはないので、署名鍵を用いてなされた電子署名に対して、事後否認防止性が弱まることはない。

【0022】次に、外部装置から入出力インターフェース2を介して、電子署名の対象となる平文に対応するデータと電子署名要求が、入出力インターフェース2を介して入力されると（図2：ステップS4）、電子署名部4bは、記憶部3から署名鍵を読み出し、この署名鍵を＊

P1=2, Q1=5

	1	2	3	4	5	6	7	8	9	10	11
1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	6	2	4	8	6	2	4	8
3	3	9	7	1	3	9	7	1	3	9	7
4	4	6	4	6	4	6	4	6	4	6	4
5	5	5	5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6	6	6	6
7	7	9	3	1	7	9	3	1	7	9	3
8	8	4	2	6	8	4	2	6	8	4	2
9	9	1	9	1	9	1	9	1	9	1	9

ED1=4n1+1
E=11, n1=8, D1=3

この表の各行は、第1列の自然数（1～9）を、1～11までべき乗した値に対しN1を法とする剰余からなっ

＊用いて入力された対象となる平文に対応するデータを暗号化する（図4（b）：①、図2：ステップS5）。そして、この暗号化されたデータ（署名データ）を、入出力インターフェース2を介して外部装置に出力する（図2：ステップS6）。なお、他のユーザは、電子署名を行ったユーザの証明書（公開鍵を含む）と、この暗号化されたデータ（署名データ）と、平文とから署名の確認を行う（図4（b）：②）。

【0023】また、公開鍵を得た外部装置により、この公開鍵を用いて平文が暗号化され（図4（c）：①）、暗号文と復号化要求が入出力インターフェース2を介して入力されると（図2：ステップS7）、復号化部4cは記憶部3から復号鍵を読み出し、入力された暗号文を復号化する（図4（c）：②、図2：ステップS8）。そして、復号化した平文を入出力インターフェース2を介して、外部装置に出力する（図2：ステップS9）。なお、ユーザが復号鍵を紛失した場合、鍵管理機関に預託した復号鍵を用いて暗号文を復号化することも、預託した復号鍵をもとに復号鍵を復元することもできる（図4（c）：③）。以上、ICカード1の動作を説明した。なお、上記で説明した動作フローは一例であり、上記の処理の流れに限定されるものではない。

【0024】次に、上記公開鍵と復号鍵と署名鍵の生成について、具体的実施例をあげ説明する。

【0025】[実施例1]以下では、RSA（Rivest Shamir Adleman）暗号方式を応用した、3つの鍵の生成例である。なお、一般に知られているRSA暗号方式の詳細については、その説明を省略する。

【0026】まず、署名鍵のもととなる相異なる2つの素数P1とQ1を任意に選択する。ここでは、P1=2、Q1=5とする。次に、P1とQ1の積であるN1を求める。

$$N1 = P1 \times Q1 = 10$$

ここで、N1=10を法とする世界は、表1のようになる。

【表1】

n1	4n1+1	D1
1	5	0.454545
2	9	0.818182
3	13	1.181818
4	17	1.545455
5	21	1.909091
6	25	2.272727
7	29	2.636364
8	33	3
9	37	3.363636

ている。これからも分かるように、各行はP1-1とQ1-1の最小公倍数（ここでは、4）の周期性をもってい

る。

【0027】ここで、署名鍵に対応する公開鍵の第1要素の候補となる自然数の列E1は、 $(P_1 - 1) \times (Q_1 - 1)$ と互いに素であり、かつ、 $4n_1 + 1$ (n_1 は、負でない整数)以外の自然数の集合として求める。ここでは、 $E_1 = \{3, 7, 11, \dots\}$ となる。

【0028】次に、復号鍵のもととなる相異なる2つの*

$P_2=3, Q_2=7$

1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	11	1	2	4	8	16	11	1	2	4	8
3	3	9	6	18	12	15	3	9	6	18	12	15	3	9	6
4	4	16	1	4	16	1	4	16	1	4	16	1	4	16	1
5	5	4	20	16	17	1	5	4	20	16	17	1	5	4	20
6	6	15	6	15	6	15	6	15	6	15	6	15	6	15	6
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
8	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8
9	9	18	15	9	18	15	9	18	15	9	18	15	9	18	15
10	10	16	13	4	19	1	10	16	13	4	19	1	10	16	13
11	11	16	8	4	2	1	11	16	8	4	2	1	11	16	8
12	12	18	6	9	3	15	12	18	6	9	3	15	12	18	6
13	13	1	13	1	13	1	13	1	13	1	13	1	13	1	13
14	14	7	14	7	14	7	14	7	14	7	14	7	14	7	14
15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15
16	16	4	1	16	4	1	16	4	1	16	4	1	16	4	1

$ED_2=6n_2+1$

$E=11, n_2=9, D_2=5$

この表の各行は、第1列の自然数(1~16)を、1~15までべき乗した値に対し N_2 を法とする剰余からなっている。これからも分かるように、各行は P_2-1 と Q_2-1 の最小公倍数(ここでは、6)の周期性をもっている。

【0029】ここで、復号鍵に対応する公開鍵の第1要素の候補となる自然数の列E2は、 $(P_2-1) \times (Q_2-1)$ と互いに素であり、かつ、 $6n_2+1$ (n_2 は、負でない整数)以外の自然数の集合として求める。ここでは、 $E_2 = \{5, 11, \dots\}$ となる。

【0030】以上で得られた、2つの秘密鍵(署名鍵、復号鍵)に共通して対応する公開鍵の第1要素の候補となる自然数の列E0が、署名鍵に対応する公開鍵の第1要素の候補となる自然数の列E1と復号鍵に対応する公開鍵の第1要素の候補となる自然数の列E2の共通部分として得られる。すなわち、

$E_0 = E_1 \cap E_2 = \{11, \dots\}$

ここで、公開鍵の第1要素Eとして1つを決定する。ここでは、 $E=11$ とする。以上により、公開鍵(E, N_1, N_2)は、 $(11, 10, 21)$ となる。

【0031】次に、等式： $E \times D_1 = \text{LCM}(P_1-1, Q_1-1) \times n_1+1$ を満たす自然数 D_1 を1つ決定し、 D_1 および N_1 の組(D_1, N_1)を署名鍵(第1の秘密鍵)とする。ここでは、 $P_1=2, Q_1=5$ 、公開鍵の第1要素Eを $E=11$ としているので、上記等式を満たす $D_1=3$ を用い、署名鍵を $(3, 10)$ とする。

【0032】次に、等式： $E \times D_2 = \text{LCM}(P_2-1, Q_2-1) \times n_2+1$ を満たす自然数 D_2 を1つ決定し、 D_2 および N_2 の組(D_2, N_2)を復号鍵(第2の秘密鍵)とする。ここでは、 $P_2=3, Q_2=7$ 、公開鍵の第1要素Eを $E=11$ としているので、上記等式を満たす

*素数 P_2 と Q_2 を任意に選択する。ここでは、 $P_2=3, Q_2=7$ とする。次に、 P_2 と Q_2 の積である N_2 を求める。

$N_2 = P_2 \times Q_2 = 21$

ここで、 $N_2=21$ を法とする世界は、表2のようになる。

【表2】

n_2	$6n_2+1$	D_2
1	7	0.636364
2	13	1.181818
3	19	1.727273
4	25	2.272727
5	31	2.818182
6	37	3.363636
7	43	3.909091
8	49	4.454545
9	55	5
10	61	5.545455
11	67	6.090909
12	73	6.636364
13	79	7.181818
14	85	7.727273
15	91	8.272727
16	97	8.818182

$D_2=5$ を用い、復号鍵を $(5, 21)$ とする。

【0033】次に、署名鍵(D_1, N_1)を用いた電子署名(署名データ)Sは、次式により算出される。ここでは、電子署名の対象となるデータをMとしている。

$S \equiv M^{D_1} \pmod{N_1}$

そして、公開鍵(E, N_1, N_2)を用いて、次式により M' を求め、 M' とMが一致することで署名を確認することができる。

$M' \equiv S^E \pmod{N_1}$

【0034】例えば、署名鍵を用い平文(2, 4, 6)を暗号化すると、署名(署名データ)は、以下のようになる。

平文	署名
2	$2^3 \pmod{10} \equiv 8$
4	$4^3 \pmod{10} \equiv 4$
6	$6^3 \pmod{10} \equiv 6$

【0035】これらの署名データに対し、公開鍵(11, 10, 21)を用いて、署名データを復号化すると、

署名	平文
8	$8^{11} \pmod{10} \equiv 2$
4	$4^{11} \pmod{10} \equiv 4$
6	$6^{11} \pmod{10} \equiv 6$

となる。

【0036】このように、署名鍵(D_1, N_1) = (3, 10)を用いて暗号化された署名データは、公開鍵(E, N_1, N_2) = (11, 10, 21)を用いて復号化できる。そして、署名データから公開鍵(E, N_1, N_2)を用いてもとの平文が得られることで、確かに公開鍵を公開した者による平文とその署名であることが確認できる。上記例で、Mとして平文のデータを用いてい

るが、例えば、電子署名の対象となる平文を、ハッシュ関数を用いて変換したものを用いてもよい。

【0037】次に、公開鍵(E, N1, N2)を用いた平文Mの暗号化は、次式により行われる。

$$C \equiv M^e \pmod{N2}$$

そして、復号鍵(D2, N2)を用いて、次式により復号化が行われる。

$$M \equiv C^{d2} \pmod{N2}$$

【0038】例えば、公開鍵を取得した者が、この公開鍵を用いて平文(2, 4, 6)を暗号化すると、以下のようになる。

平文 暗号文

$$2 \quad 2^{11} \pmod{21} \equiv 11$$

$$4 \quad 4^{11} \pmod{21} \equiv 16$$

$$6 \quad 6^{11} \pmod{21} \equiv 6$$

【0039】そして、この暗号文は、復号鍵を用いて以下のように復号化される。

暗号文 平文

$$11 \quad 11^5 \pmod{21} \equiv 2$$

$$16 \quad 16^5 \pmod{21} \equiv 4$$

$$6 \quad 6^5 \pmod{21} \equiv 6$$

【0040】このように、公開鍵(E, N1, N2) = (11, 10, 21)を用いて暗号化された暗号文は、復号鍵(D2, N2) = (5, 21)を用いて復号化できる。以上のようにして、1つの公開鍵と、署名鍵と、復号鍵とを生成することができる。

【0041】従来のRSA暗号方式では、上記で説明した(E, N1)の組で署名鍵に対応する公開鍵をなし、また、(E, N2)の組で復号鍵に対応する公開鍵をなすが、本実施例では、(E, N1, N2)の組で1つの公開鍵を構成している。こうすることで、2つの公開鍵(E, N1)および(E, N2)を用いるよりも、鍵のデータ長を短くすることができる。また、公開鍵を2つ管理する必要がなくなる。

【0042】[実施例2]以下では、ElGamal暗号方式を応用した、3つの鍵の生成例である。なお、一般に知られているElGamal暗号方式の詳細については、その説明を省略する。

【0043】本実施例で用いる、1つの公開鍵(g, p, T1, T2)と、署名鍵(g, p, S1)と、復号鍵(g, p, S2)との間には、次式の関係をもつ。

$$g^{S1} \pmod{p} \equiv T1$$

$$g^{S2} \pmod{p} \equiv T2$$

ただし、pは素数である。以下では、g=4、p=5、S1=2、T1=1、S2=3、T2=4として、説明する。この場合、公開鍵は(4, 5, 1, 4)の組となり、署名鍵は(4, 5, 2)の組となり、復号鍵は(4, 5, 3)の組となる。

【0044】(1)電子署名について

メッセージmとこのメッセージmの電子署名の組を

(m, X, Tm)とすると、以下の式に示される関係をもつ。

$$Tm \equiv g^x \pmod{p}$$

$$dm = MD(m, Tm)$$

$$X \equiv R + dm \times S1 \pmod{p-1}$$

ただし、MD()は、メッセージダイジェスト関数(ハッシュ関数)であり、MD(m, Tm)は、mとTmを連結したもののハッシュ値である。

【0045】以下では、説明を簡単にするため、電子署名をするメッセージmとしてm=3、MD(m, Tm)が3になったと仮定しdm=3、乱数RとしてR=4を用いるものとする。このとき、

$$Tm \equiv g^x \pmod{p} = 4^x \pmod{5} \equiv 1$$

$$dm = MD(m, Tm) = 3$$

$$X \equiv R + dm \times S1 \pmod{p-1} \equiv 2$$

となり、メッセージとその署名の組は、(3, 2, 1)となる。

【0046】この電子署名の確認は、次式が一致することにより行われる。

$$g^x \pmod{p} = 4^2 \pmod{5} \equiv 1$$

$$Tm \times T1^{d^*} \pmod{p} = 1 \times 1^3 \pmod{5} \equiv 1$$

上記例では、上記2つの式の値が一致しているため、署名が正当なものであることが確認される。

【0047】(2)暗号化・復号化について

メッセージmに対する暗号文(C1, C2)は、次式の関係をもつ。

$$C1 \equiv g^m \pmod{p}$$

$$C2 \equiv m \times T2^x \pmod{p}$$

ここでも、説明を簡単にするため、暗号化をするメッセージmとしてm=3、乱数RとしてR=4を用いるものとする。このとき、

$$C1 \equiv 4^3 \pmod{5} \equiv 1$$

$$C2 \equiv 3 \times 4^4 \pmod{5} \equiv 3$$

となり、メッセージm=3に対する暗号文(C1, C2)は、(1, 3)となる。

【0048】この暗号文(C1, C2)に対し、復号化は次式で行える。

$$m \equiv C2 / (C1^{S2}) \pmod{p}$$

$$= 3 / (1^3) \pmod{5}$$

$$\equiv 3$$

このように、公開鍵(g, p, T1, T2) = (4, 5, 1, 4)を用いて暗号化された暗号文は、復号鍵(g, p, S2) = (4, 5, 3)を用いて復号化できる。以上のようにして、1つの公開鍵と、署名鍵と、復号鍵とを生成することができる。

【0049】次に、公開鍵の実装例について説明する。

一般に、公開鍵は、認証局により発行される証明書(デジタル証明書)に含められ利用される。この証明書のフォーマットとして、国際標準であるITU-TX. 509が利用される。従来のRSA暗号方式では、公開鍵は

2つの構成要素からなる。例えば、上記実施例1の場合、従来のRSA暗号方式による公開鍵は、(E, N1)の組または(E, N2)の組となる。一般に利用されている証明書には、RSA暗号方式の場合、2つ構成要素からなる公開鍵がX. 509のフォーマットで格納され利用される(図5(a)参照)。

【0050】一方、本発明に基づく実施例1では、(E, N1, N2)の組で1つの公開鍵を構成している。そこで、本実施例では、X. 509v3(バージョン3)において規定される拡張領域(エクステンション・フィールド)を利用し、公開鍵の第2要素N1または第3要素N2を、この拡張領域に含めるように実装する。このように実装すると、拡張領域に格納されていない公開鍵のデータは、署名鍵または復号鍵のいずれかに対応する公開鍵として、X. 509に対応した既存システムのAPI(Application Programming Interface)を用いて利用できる。ただし、拡張領域にある公開鍵のデータの一部(N1またはN2)にアクセスするためには、そのための拡張APIを別途用意する必要がある。以下に説明する実施例1および実施例2は、実施例1の公開鍵(E, N1, N2)の実装を、このX. 509のフォーマットに適用するのである。

【0051】[実装例1] 本実施例では、X. 509v3で規定されている拡張領域を利用して、この拡張領域に公開鍵の第3要素N2を格納し、公開鍵の第1要素Eと署名鍵に対応する第2要素N1は、基本領域に格納する(図5(b)参照)。この場合、既存APIを用いて、拡張領域ではない領域に格納された、公開鍵の第1要素Eと署名鍵に対応する第2要素N1にアクセスできる。したがって、既存APIでは、公開鍵と署名鍵を使った暗号化・復号化および電子署名を行える。しかし、既存APIによる暗号化を行った場合、署名鍵に対応する公開鍵で暗号化することになるので、署名鍵を紛失した場合、暗号文の復号化が不可能となる。

【0052】本実施例では、電子署名を、既存APIを用いて行い、暗号化は、拡張領域にもアクセス可能な拡張APIを別途用意し、基本領域にある公開鍵の第1要素Eと拡張領域にある復号鍵に対応する第3要素N2を用いて暗号化を行う。そして、復号鍵は、別途、鍵管理機関に預託をする。このようにして、復号鍵が紛失しても、この復号鍵は別途預託してあるので、暗号文を復号化できなくなることはない。

【0053】[実装例2] 本方式では、X. 509v3で規定されている拡張領域を利用して、この拡張領域に公開鍵の第3要素N1を格納する(図5(c)参照)。この場合、既存APIを用いて、拡張領域ではない領域に格納された、公開鍵の第1要素Eと復号鍵に対応する第3要素N2にアクセスできる。したがって、既存APIでは、公開鍵と復号鍵を使った暗号化・復号化および

電子署名を行える。そして、復号鍵を、別途鍵管理機関に預託しておけば、この復号鍵が紛失しても暗号文を復号化できなくなることはない。しかし、既存APIによる電子署名を行った場合、預託した復号鍵で電子署名をすることになるので、この電子署名に対する事後否認が可能となってしまう。

【0054】本実施例では、公開鍵による暗号化を、既存APIを用いて行い、電子署名は、拡張領域にもアクセス可能な拡張APIを別途用意し、基本領域にある公開鍵の第1要素Eと拡張領域にある署名鍵に対応する第2要素N1を用いて、署名鍵を用いてなされた電子署名の確認を行う。こうすることで、電子署名に対する事後否認を防ぐことができる。以上、公開鍵の実装例を説明した。

【0055】以上では、1つの公開鍵と、署名鍵と、復号鍵からなる3つの鍵を用いているが、署名鍵と復号鍵に対応する公開鍵をそれぞれ用意し、2つの公開鍵と、署名鍵と、復号鍵からなる4つの鍵を用いるようにしてもよい。

【0056】なお、図1における電子署名部4bおよび復号化部4cの機能を実現するためのプログラムと公開鍵および署名鍵および復号鍵のデータ、あるいは、鍵生成部4a電および電子署名部4bおよび復号化部4cの機能を実現するためのプログラム、をコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することによりデータセキュリティ装置を実現させてもよい。なお、ここでいう「コンピュータシステム」とは、OSや周辺機器等のハードウェアを含むものとする。

【0057】また、「コンピュータ読み取り可能な記録媒体」とは、フロッピー(登録商標)ディスク、光磁気ディスク、ROM、CD-ROM等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ(RAM)のように、一定時間プログラムを保持しているものも含むものとする。

【0058】また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク(通信網)や電話回線等の通信回線(通信線)のように情報を伝送する機能を有する媒体のことをいう。また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録され

ているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

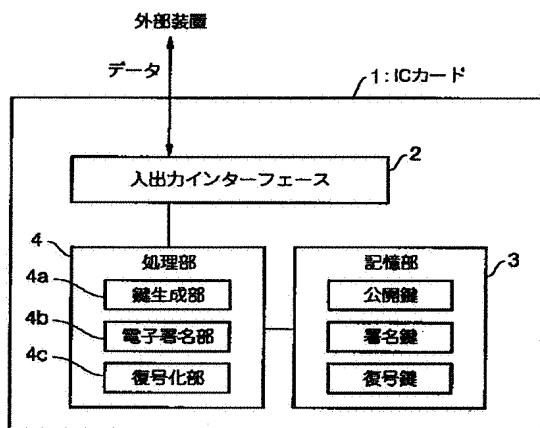
【0059】以上、この発明の実施形態を、図面を参照して詳述してきたが、具体的な構成はこれらの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【0060】

【発明の効果】以上、詳細に説明したように、本発明によれば、公開鍵方式による、電子署名に用いる第1の秘密鍵と、暗号文の復号化に用いる第2の秘密鍵を異なるようにしたので、電子署名用の第1の秘密鍵と復号化用の第2の秘密鍵とを別々に管理することができる。したがって、電子署名に用いる第1の秘密鍵を秘密に管理することで、電子署名の事後否認を防止できる。そしてさらに、復号化に用いる第2の秘密鍵を鍵を管理する機関に預託することで、第2の秘密鍵の所有者が自身が所有している第2の秘密鍵を紛失しても、預託した第2の秘密鍵を利用することで、対応する公開鍵で暗号化された暗号文の復号化を行うことができる。また、第1および第2の秘密鍵に対応する公開鍵を共通にしたので、公開鍵の管理を統一的行える。すなわち、公開鍵を2つ管理する必要がなくなる。また、公開鍵を2つした場合に比べ、公開鍵のデータ長を短くすることができる。

【0061】また、公開鍵と第1の秘密鍵と第2の秘密鍵をICカード内にもち、公開鍵と第2の秘密鍵を外部に出力し、電子署名用の第1の秘密鍵をICカードから外部に出力しないので、第3者は、ICカードから出力された公開鍵を用いて、ICカード内の第1の秘密鍵でなされた電子署名の確認を行え、また、このICカードが破損ないし紛失しても、外部に出力された第2の秘密*

【図1】



* 鍵を用いることで、公開鍵を用いて暗号化された暗号文の復号化が行える。

【0062】また、公開鍵の電子証明書において、公開鍵の3つの要素の内、第2要素N1と第3要素N2の一方を、ITU-T X.509バージョン3の拡張領域に格納して利用するので、他方の要素と公開鍵の第1要素Eは、X.509に対応した既存のシステムでも利用可能となる。

【図面の簡単な説明】

10 【図1】 本発明の一実施の形態であるデータセキュリティ装置（ICカード）の構成を示すブロック図である。

【図2】 同実施の形態の動作フローチャートの例である。

【図3】 同実施の形態の利用例を示す図である。

【図4】 (a) 鍵生成／公開鍵の公開／復号鍵の預託を示す図、(b) 署名／署名の確認を説明する図、(c) 暗号化／復号化／復号鍵の復元を説明する図である。

20 【図5】 (a) X.509フォーマットにおける従来の公開鍵の格納形式を説明する図、(b) 本発明の一実施の形態の公開鍵の一実装例を説明する図、(c) 同実施の形態の公開鍵の他の実装例を説明する図である。

【図6】 従来の公開鍵方式の問題点を説明する図である。

【符号の説明】

1…ICカード（データセキュリティ装置）

2…入出力インターフェース

3…記憶部

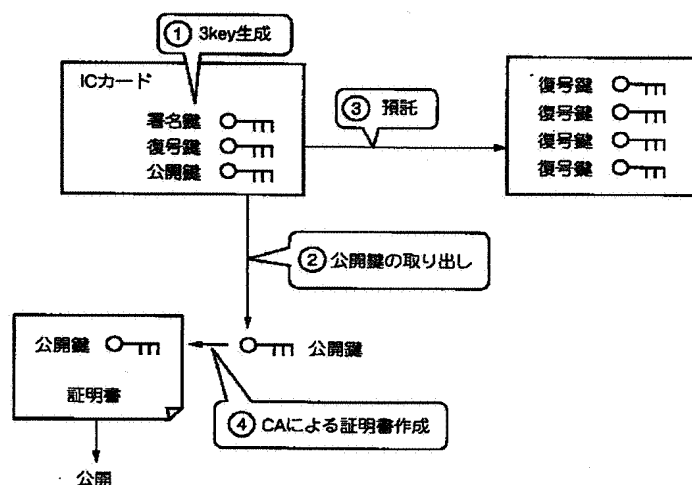
4…処理部

4a…鍵生成部

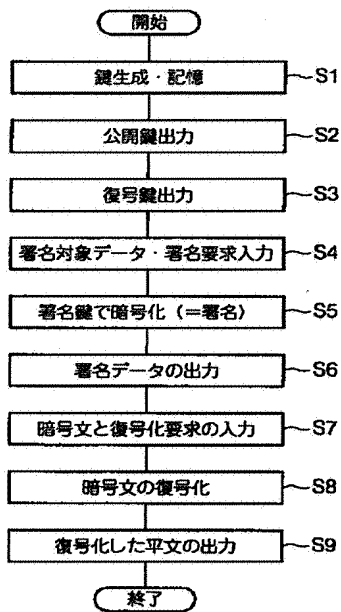
30 4b…電子署名部

4c…復号化部

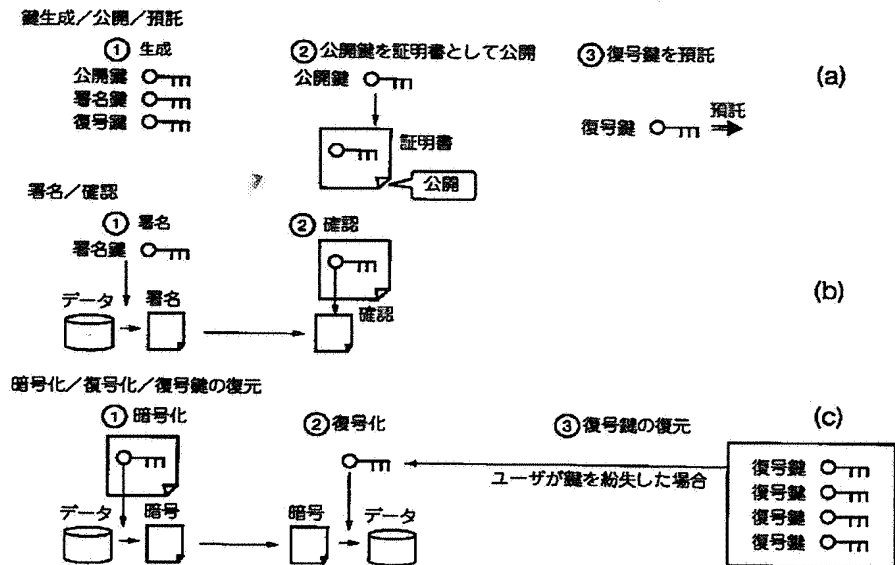
【図3】



【図2】



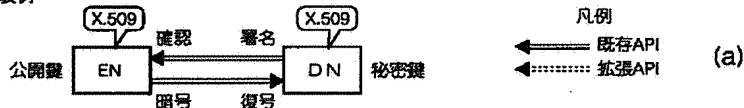
【図4】



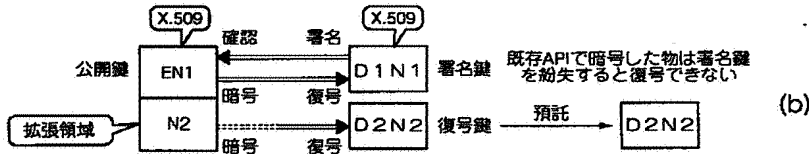
【図5】

APIと証明書フォーマット

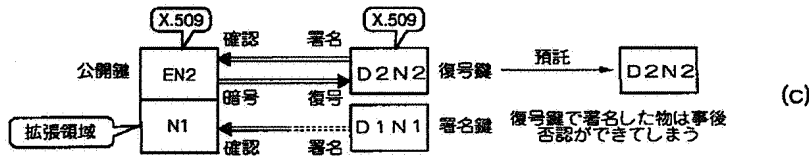
従来の実装例



N2を拡張領域に入れる実装例 (実装例1)



N1を拡張領域に入れる実装例 (実装例2)



【図6】

従来の公開鍵方式

